REMARKS

In the Official Action mailed on **March 16, 2004**, the examiner reviewed claims 1-33. Claims 1-33 were rejected under 35 U.S.C. 102(e) as being anticipated by Boneh, et al. (USPN 6,134,660, hereinafter "Boneh"). In the advisory action mailed on **May 19, 2004,** the Examiner avers "Applicant's 'information system' is the backup system of Boneh..."

Rejections under 35 U.S.C. §102(e)

Independent claims 1, 12, and 23 were rejected as being anticipated by Boneh. Applicant respectfully points out that Boneh teaches **deleting backup data** by deleting an encryption key used to encrypt the backup data (see Boneh, col. 3, lines 5-27). The system of Boneh, however, leaves the **local persistent file unencrypted** (see Boneh, FIG. 2, index 202, and col. 4, lines 17-22). The local persistent file, therefore, cannot be deleted by deleting the encryption key.

In contrast, the present invention encrypts **all copies** of information, **including the local persistent file** (see FIG. 2 and page 10, lines 7-24 of the instant application). There is nothing within Boneh, either explicit or implicit, which suggests encrypting all copies of information, including the local persistent file, so that deleting the encryption key ensures that the set of information is not available within the system. In fact, Boneh teaches away from encrypting the local persistent file (see Boneh, col. 10, lines 50-51 "The system preferably requires no modification to existing file systems.")

The Examiner avers "Applicant's 'information system' is the backup system of Boneh..." Applicant respectfully points out that the present invention refers to a complete "information system," which encrypts an information set when the information set enters the information system prior to storing the information set in the information system (see page 2, line 22 to page 3, line 2 of the instant application). The unencrypted form of the information set is **not**

because storing a non-encrypted form can compromise security. This information system is the overall entity responsible for storing and maintaining information sets (see page 5, lines 10-11 of the instant application). All information sets are encrypted prior to storing the information set into a repository (see page 6, lines 8-11 of the instant application).

In the system of Boneh, the files 202 are clearly not encrypted (see Boneh, FIG. 2, index 202, and col. 4, lines 17-22), and, therefore, cannot be rendered unavailable by deleting the encryption key. Thus the system of Boneh does not provide the ability to purge information by deleting an encryption key because the files 202 are still available after the encryption key has been deleted.

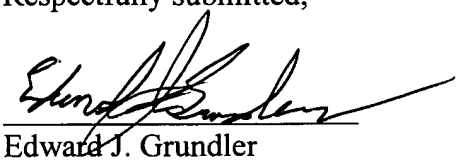
Accordingly, Applicant has amended independent claims 1, 12, and 23 to clarify that the present invention encrypts all copies of information, including the local persistent file, so that deleting the encryption key ensures that the information is not available within the system.

Hence, Applicant respectfully submits that independent claims 1, 12, and 23 as presently amended are in condition for allowance. Applicant also submits that claims 2-11, which depend upon claim 1, claims 13-22, which depend upon claim 12, and claims 24-33, which depend upon claim 23, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47, 615

Date: May 27, 2004

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
508 Second Street, Suite 201
Davis, CA 95616-4692
Tel: (530) 759-1663
FAX: (530) 759-1665